EXHIBIT 5

Progress in the Privacy Sandbox (November 2021)

Welcome to the November edition of Progress in the Privacy Sandbox, tracking the milestones on the path to phasing out third-party cookies in Chrome and working towards a more private web. Each month we'll share an overview of the updates to the **Privacy Sandbox timeline** (https://privacysandbox.com/timeline/) along with news from across the project. We've also provided an update on our Privacy Sandbox commitments (https://blog.google/around-the-globe/google-europe/update-our-privacy-sandbox-commitments/) as we ensure proposals are designed, developed and implemented with regulatory oversight and input from the UK's Competition and Markets Authority (CMA) and Information Commissioner's Office (ICO).

Note: As we approach the end of the year there are fewer changes across the different proposals, so the update here is also lighter. However, this does mean it's a good time for testing and addressing questions, which we are always happy to hear about either on the @ChromiumDev Twitter (https://twitter.com/ChromiumDev) or the developer support repo (https://github.com/GoogleChromeLabs/privacy-sandbox-dev-support).

Events

At the beginning of November we hosted the Chrome Developer Summit, which included both a Privacy Sandbox segment in the keynote and a few related questions in the Ask Me Anything (AMA) session. We've added a summary for you (/privacy-sandbox/archive/cds21-update) to read or watch that covers activities and examples of what to expect as proposals progress through the discussion, testing, and scaled adoption phases.

Strengthen cross-site privacy boundaries

Third-party cookies are a key mechanism that enables cross-site tracking. Phasing them out is a major milestone, but we also need to tackle other forms of cross-site storage or communication.

Federated Credentials Management API

Federated Credentials Management (FedCM) (https://github.com/WICG/FedCM) is the new, more meaningful name for the WebID proposal. We've reflected this change in the Privacy Sandbox Timeline (https://privacysandbox.com/timeline/). Federated identity is a critical service for the web, but given that it's explicitly used to share aspects of identity across other sites, there are implementation details which overlap with cross-site tracking.

The Federated Credentials Management proposal explores a range of options: from simple migration paths for existing solutions to more private methods of connecting to services with the bare minimum of information shared.

November also included the bi-annual **BlinkOn** (https://www.chromium.org/events/blinkon-15) conference. Blink is the rendering engine used by Chromium, and BlinkOn is where contributors gather for engineering presentations and discussions on current projects. The November BlinkOn included an **overview and Q&A session on FedCM**: you can watch the recording on YouTube (https://www.youtube.com/watch?v=9la0cBhVXac).

Preventing covert tracking

As we reduce the options for explicit cross-site tracking, we also need to address the areas of the web platform that expose identifying information which enables fingerprinting or covert tracking of users.

User-Agent string reduction and User-Agent Client Hints

Progress continues on reducing the information available by default in Chrome's User-Agent string and providing an improved, active method for requesting that data via User-Agent Client Hints. We've added a new **User-Agent Reduction** (/privacy-sandbox/protections/user-agent) **overview** to collate all the current guidance and updates.

We published new testing resources to help prepare for the changes. The User-Agent reduction code snippets provide a selection of examples for transforming the current Chrome User-Agent string to the reduced format. There is also the new `chrome://flags/#force-major-version-to-100` entry which will let you check if the switch to a 3 digit major version causes your site to malfunction or break.

We have published the **Intent to Ship for Sec-CH-UA-Full-Version-List** (https://groups.google.com/a/chromium.org/g/blink-dev/c/yZh8Lwr34Ro). This addresses ecosystem feedback (https://github.com/WICG/ua-client-hints/issues/196) that the existing Sec-CH-UA-Full-Version was too tightly bound to the primary browser brand as it only provided a single value. For example, the current implementation shows:

↓ *Server response header*

```
Accept-CH: Sec-CH-UA-Full-Version
```

↑ *Browser request header*

```
Sec-CH-UA: "Chromium";v="94", "Google Chrome";v="94", ";Not A Brand";v="99"
Sec-CH-UA-Full-Version: "94.0.4606.124"
```

The updated version would provide:

↓ *Server response header*

```
Accept-CH: Sec-CH-UA-Full-Version-List
```

⬆ *Browser request header*

```
Sec-CH-UA: "Chromium";v="94", "Google Chrome";v="94", "Other browser";v="99"
Sec-CH-UA-Full-Version-List: "Chromium";v="94.0.4606.124", "Google Chrome";v="94
```

Note: If you are using **`Sec-CH-UA-Full-Version`** then you should plan to migrate to **`Sec-CH-UA-Full-Version-List`** as it will allow us to deprecate **`Sec-CH-UA-Full-Version`** in the future.

IP blindness

IP addresses by their nature often provide a unique identifier for a client enabling the necessary communication between browser and server. However, this also means that a stable IP address over time passively provides a significant amount of information that can be used for cross-site tracking.

The **IP blindness proposal** (https://github.com/bslassey/ip-blindness) (also known as Global Network Address Translation Combined with Audited and Trusted CDN or HTTP-Proxy Eliminating Reidentification or **Gnatcatcher**) details a two pronged approach to addressing this issue. The first is Near-Path NAT (https://github.com/bslassey/ip-blindness/blob/master/near_path_nat.md) which effectively forwards the browser's connection through an IP privatizing service which hides the browser's IP address from the site being visited. The second option builds on the layered nature of the Internet where the infrastructure that relies on IP address can be wholly separate from the application running on top of it. The Willful IP Blindness (https://github.com/bslassey/ip-blindness/blob/master/willful_ip_blindness.md) proposal explores methods of defining auditable policies for creating and maintaining that separation.

Both of these ideas are early in the discussion phase with active progress in the repo, such as the recently posted Willful IP Blindness Principles (https://github.com/bslassey/ip-blindness/blob/master/proposed_willful_ip_blindness_principles.md). You can expect to see discussion continue there and if you're interested in the network-level details,

you can follow the Multiplexed Application Substrate over QUIC Encryption (MASQUE) (https://datatracker.ietf.org/wg/masque/about/) Working Group in the IETF.

Measure digital ads

As the companion to displaying ads without cross-site tracking, we need privacy-preserving mechanisms to allow measurement of ad effectiveness.

Attribution Reporting API

The **Attribution Reporting API** (/privacy-sandbox/relevance/attribution-reporting) creates functionality to measure events on one site, like clicking or viewing an ad, that lead to a conversion on another site—without enabling cross-site tracking.

We continue to test the API and **the origin trial has been extended** (https://groups.google.com/a/chromium.org/g/blink-dev/c/DdjaFmsb4fA) through to Chrome 97. Current origin trial tokens expired on October 12th, so existing testers need to apply for updated tokens to continue testing.

There are two new blog posts up with the latest details on event-level reporting in the API. **Event-level reports in the Attribution Reporting API** (/privacy-sandbox/relevance/attribution-reporting#event-level_reports) introduces the concepts and process while **Using event-level reports in the Attribution Reporting API** (/privacy-sandbox/relevance/attribution-reporting/attribution-reporting-experiment) goes into the implementation detail with accompanying demo and demo code.

Feedback

As we continue to publish these monthly updates, and progress through the Privacy Sandbox as a whole, we want to make sure that developers receive the information and support that they need. Let us know on @ChromiumDev Twitter (https://twitter.com/ChromiumDev) if there's anything that we could improve in this series. We'll use your input to continue improving the format.

Check out the **Privacy Sandbox FAQ** (/privacy-sandbox/overview/faq), which we continue to expand based on the issues you submit to the developer support repo

(https://github.com/GoogleChromeLabs/privacy-sandbox-dev-support). If you have any questions around testing or implementation on any of the proposals, come talk to us there.

Last updated 2021-11-30 UTC.